REMARKS

Claims 1-3, 5, 6, 8-10, 12, 14, 15, 17, 28-31, 41, 42, 44, 45, and 47-56 are currently pending. Claims 4, 7, 16, 23-27, 32-40, 43, and 46 have been cancelled without prejudice or disclaimer. Claims 1, 10, 12, 23, 28, and 34 have been amended for clarification purposes only and are self-supporting and supported also by the subject matter of the cancelled claims, page 5, lines 23-28, and page 6, line 5, through page 7, line 22, of the specification as filed, and Figures 3 and 6, as well as elsewhere in the original disclosure. Claims 50-56 have been added to enhance the scope of Applicant's patent coverage and are supported by the original claims, page 5, lines 23-28, and page 6, line 5, through page 7, line 22, of the specification as filed, and Figures 3 and 6, as well as elsewhere in the original disclosure. It is respectfully submitted that no new matter has been added.

Applicant has amended the claims to advance prosecution and does not explicitly or implicitly admit a need for amendment of the claims.

The Patent Office rejected claims 1, 3, 5, 6, 10, 23, 26, 42, 44, 45, and 49 under 35 U.S.C. 103(a) as being unpatentable over Nagaoka, U.S. Published Patent Application No. 2002/0092024, in view of Ching, U.S. Patent No. 7,222,354.

Although the claims stand on their own, for the purposes of certain aspects of the claimed invention, claim 1 will now be discussed. Claim 1 defines encrypting message detection data comprising an address (for instance an email address) and a key (a decryption key, which is associated only with the address) with a key that is substantially unique to a digital broadcast receiver. As such, the message detection data can be decrypted only by the digital broadcast receiver that possesses the unique key (for instance because it is provided with the key at manufacture). Following decryption of the encrypted message detection data, the digital broadcast receiver stores the message detection data (i.e. the address and associated key). This configures the digital broadcast receiver in the sense that it then has the information required to be able to receive messages addressed to the digital broadcast receiver (the address is associated with the digital broadcast receiver by way of the message detection data) and to decrypt those messages (using the key associated with the address).

The features of the method of claim 1 allow configuration of the digital broadcast receiver over-the-air. Since the message detection data is encrypted with a unique key associated with the

digital broadcast receiver, the message detection data cannot be decrypted by any other receiver. Furthermore, since the content of subsequent messages is encrypted using a key forming part of the message detection data (and since no other digital broadcast receiver has this message detection data or the key), it is only the correct digital broadcast receiver that can decrypt and thus render messages which are subsequently addressed to the address. This provides protection against subsequent interception by other receivers of messages intended for the digital broadcast receiver. Importantly, this is achieved without the need for the digital broadcast receiver to be configured at manufacture or at point-of-sale; instead, configuration can be achieved through a broadcast of the encrypted message detection data.

Nagaoka discloses a method and a broadcast system for provision of a program enabling a large number of widely dispersed viewers to participate in the program while maintaining a real time feeling therein – see paragraphs [0006] and [0037]. The broadcasting system comprises a plurality of mobile phones 1A, 1B, ..., a broadcast station 2, a transaction management system (TMS) 3, a plurality of set top boxes (STBs) 4 and a mobile packet communication network 5 – see Figure 1 and [0036]. The TMS 3 receives data broadcast by the broadcast station 2 and converts it to a format of data that is displayed by the mobile phones 1 – see paragraphs [0047] and [0049]. The STB 4 also receives and displays the broadcast data – see [0044] and [0045]. The mobile phones 1 have memories which store sender Ids which are for identifying the mobile phones 1 in the mobile packet communication network 5, for participation in the program and for verifying users' identities effectively to prevent an identity theft – see [0053], [0084], [0087], [0092], and [0142]. From [0037], it can be seen that Nagaoka aims to enable users of the mobile phones 1 to participate in an auction program broadcast by station 2. Indeed, this is confirmed as the core of the disclosure of that document by [0057], [0140] and so on.

Considering the STB 4 of Nagaoka to be the digital broadcast receiver of claim 1 (as asserted by the Patent Office), Nagaoka does not disclose (as has been claimed) "sending to [the STB4] through a digital broadcast network message detection data that allows the [STB 4] to identify messages broadcast through said digital broadcast network with at least one individual address corresponding to the [STB 4]". Instead the STB 4 simply receives program data (including a program code), report information data (e.g., text indicating the current bid in a program) and electrical program guide data – see [0038], [0040].

Indeed, Nagaoka does not relate to configuring a digital broadcast receiver at all.

Furthermore, none of the data sent to the STB 4 in Nagaoka "is encrypted using a key associated substantially uniquely with said digital broadcast receiver", as is recited by claim 1. Indeed, none of the data seems to be signed at all, let alone with a key associated with the STB 4.

The STB 4 of Nagaoka appears identical to all of the other STBs in the system. See, for example, paragraph 0036. The STB 4 receives signals broadcast by a broadcast station 2. However, the digital broadcast receiver does not have an address associated with it, and is unable to detect messages addressed to it. The mobile phone 1 can be addressed, but the mobile phone 1 and the STB 4 are entirely different. Indeed, they are unconnected parts of the system. There is not even any communication between the STB 4 and the mobile phone 1. Some information is displayed through the SJTB 4 and through the mobile phone 1 (see paragraph 0049), but there is where the similarity ends.

It is not reasonable to assert that what Nagaoka teaches in relation to the mobile phones is applicable also to the set top box. Consequently, the STB 4 of Nagaoka does not constitute the features of claim 1 alleged by the Patent Office to be constituted by the STB 4 of Nagaoka.

The Patent Office noted that Nagaoka has more deficiencies that teachings of the claimed invention by writing that Nagaoka teaches "As to claims 1, 10, and 23, Nagaoka teaches a method and an apparatus comprising: sending to a digital broadcast receiver ([0044]) where the messages comprise at least one of meassages derived from a different network ([0061]) and messages emanating from a different network ([0061])" and then lists the deficiencies of Nagaoka as follows:

> However, Nagaoka fails to disclose message detection data that allows said digital broadcast receiver to identify messages broadcast through said digital broadcast network in at least one individual address corresponding to said digital broadcast receiver, storing said message detection data for use in said digital broadcast receiver to detect messages addressed thereto, wherein said message detection data comprises at least one of message detection data including identity data corresponding to an individual identification code of configuring said digital broadcast receiver to receive individually addressed messages through said broadcast network.

The passages of column 3, lines 4-8, and column 5, lines 16-35, of Ching have been cited by the Patent Office as providing the teachings to correct the alleged deficiencies of Nagaoka.

These passages have been reproduced immediately below and clearly provide none of the alleged teachings.

> FIGS. 6A and 6B are a flow diagram of the viewer unit of FIG. 5 inserting multimedia segments, according to the present invention. FIG. 7 is a flow diagram of the creation of the play-list at a head-end of FIG. 1 according to the present invention.
> Embodiment of Providing Customized Advertisement
> FIG. 2 shows receiving groups in the neighborhood comprising homes 4-9. Group 20 is composed of houses 4 and 9; group 21 is composed of houses 7, 5, and 4; and group 22 is composed of houses 6 and 4. Group advertising is the delivery of multimedia segments and play-lists to members of a group. By way of example, group 20 is "addressed" by a beer company to advertise its major brand. The advertising agency of the beer company contracts with the cable company to show 100 impressions of a beer ad to houses 4 and 9. The advertising agency has already determined a high likelihood of beer consumers in households 4 and 9, and therefore contracts with the cable company to deliver their beer commercial to optimize for maximum effectiveness in encouraging beer purchase in those households. Similarly group 22 has been "addressed" by a diaper company to advertise its major brand. The advertising agency of the diaper company contracts with the cable company to show 30 impressions of a diaper ad to houses in group 22, having determined that 30 is the optimum number of repetitions to encourage diaper purchase in homes with infants.

It is clear that, like Nagaoka, Ching does not teach or suggest sending message detection data having the contents claimed for the message detection data in claim 1. Furthermore, like Nagaoka, Ching, does not disclose or suggest using a key obtained from decrypting message detection data to decrypt subsequently received messages. It is not seen where in either Nagaoka or Ching there is a teaching or suggestion of claimed subject matter of either "message detection data also comprising, for each individual address, at least one associated key" or "said message detection data is encrypted using a key associated substantially uniquely with said digital broadcast receiver."

Claims 10 and 50 are apparatus and method claims, respectively, and directed to the digital broadcast receiver aspects of claim 1. As such, these claims are patentable for corresponding reasons. Claims 12 and 28 are apparatus and method claims, respectively, and are

directed to the digital broadcast network aspects of claim 1. As such, these claims are patentable for reasons corresponding to those given for claim 1.

According, all claims 1-3, 5, 6, 8-10, 12, 14, 15, 17, 28-31, 41, 42, 44, 45, and 47-56 are allowable over the combination of Nagaoka and Ching.

The Patent Office rejected claims 4, 7, 9, 12, 14, 16, 17, 24, 27, 28, 31-34, 36-40, 43, 46, and 48 under 35 U.S.C. 103(a) as being unpatentable over Nagaoka, U.S. Published Patent Application No. 2002/009024, in view of Ching, U.S. Patent No. 7,222,354, and further in view of Syed, U.S. Patent No. 6,845,230.

Where does Nagaoka, Ching, or Syed disclose "said message detection data comprising at least one individual address corresponding to said digital broadcast receiver and, for each individual address, at least one associated key?" From the Office Action dated October 20, 2006, it appears that the Patent Office considers column 13, line 66, through column 4, line 6, of Syed, to provide such a teaching as the Patent Office alleges that Syed teaches "said message detection data includes a decryption key corresponding to said address, said decryption key being for decoding encrypted messages sent to said address at said digital broadcast key" and further considers Syed to discuss including "encryption key in the data and the receiver would use the key to decrypt the data." This position is repeated in the January 11, 2008, Office Action by the Patent Office, relying again on the passage from column 3, lines 66, through column 4, line 6, of Syed. However, **this passage of Syed cited by the Patent Office does not teach the claimed subject matter of "for each individual address, at least one associated key."**

None of the prior art of record discloses sending message detection data having the contents claimed for the message detection data in claim 1. Furthermore, none of the prior art of record discloses using a key obtained from decrypting message detection data to decrypt subsequently received messages. As such, the prior art of record does not render claim 1 to be obvious.

Thus, claims 4, 7, 9, 12, 14, 16, 17, 24, 27, 28, 31-34, 36-40, 43, 46, and 48 are allowable over a combination of Nagaoka, Ching, and Syed.

The Patent Office rejected claims 15, 29, 30, and 35 under 35 U.S.C. 103(a) as being

unpatentable over Nagaoka, Ching, and Syed as applied to claims 12, 28, and 34 above, and further in view of Thornton.

Thornton (U.S. published patent application no. 2003/0056220) concerns enabling users with independent terminal devices to share audiovisual content in the context of a communication session, shared software application, or common experience – see paragraph [0002].

The Patent Office asserts that Syed discloses "message detection data which is encrypted using a substantially unique key associated with the digital receiver." However, the passage referred to (i.e., the paragraph spanning columns 13 and 14) discloses only an encryption public key, and does not disclose "a substantially unique key associated with said digital receiver." Conversely, Syed does not relate to individually addressing broadcast receivers, so Syed does not need to provide a key substantially unique to a digital receiver. Instead, it would seem that the broadcast of a public key by the stem of Syed results in broadcasts being encrypted only be receivers which are authorized to receive broadcasts. The provision of a suitable key to those receivers would allow them to decode encrypted broadcasts but would prevent other receivers being able to decode encrypted broadcasts.

As none of Nagaoka, Ching, Syed, or Thornton discloses "said message detection data comprising at least one individual address corresponding to said digital broadcast receiver and, for each individual address, at least one associated key," any combination of Nagaoka, Ching, Syed, and Thornton would not make obvious any of claims 15, 29, 30, and 35.

The Patent Office rejected claims 2, 15, 25, 29, 30, 35, and 41 under 35 U.S.C. 103(a) as being unpatentable over Nagaoka in view of Ching as applied to claims 1, 10 and 23 above and further in view of Thornton, U.S. Published Patent Application No. 2003/0056220.

Thornton (U.S. published patent application no. 2003/0056220) concerns enabling users with independent terminal devices to share audiovisual content in the context of a communication session, shared software application, or common experience – see paragraph [0002].

None of the prior art of record discloses sending message detection data having the contents claimed for the message detection data in claim 1. Furthermore, none of the prior art of record discloses using a key obtained from decrypting message detection data to decrypt

subsequently received messages.

For the reasons discussed above, none of claims 2, 15, 25, 29, 30, 35, and 41 are obvious in view of Nagaoka, Ching, and Thornton, alone or in combination.

The Patent Office rejected claims 8 and 47 under 35 U.S.C. 103(a) as being unpatentable over Nagaoka and Syed as applied to claim 1 and 10 above, and further in view of Mathis, U.S. Patent No. 6,993,327.

First, claims 1 and 10 were rejected by a combination of Nagaoka and Ching, not Nagaoka and Syed. The deficiency the Patent Office has noted in Nagaoka discussed on page 3, lines 1-9, of the January 11, 2008, Office Action, is not treated or remedied by Syed as discussed, for example, on page 8, lines 1-8, of the January 11, 2008, Office Action.

Second, Mathis does not remedy the deficiency of Nagaoka and Ching (or, Syed). Mathis discloses (column 5, lines 28-35):

> Upon receiving one or more multicast addresses, each client device 102, 104, 106, 108 performs actions necessary, i.e., configures itself, to receive multicast traffic sent to these multicast addresses at Step 260. The preferred embodiment is based on IP Multicast and, thus, each client device 102, 104, 106, 108 sends an Internet Group Management Protocol ("IGMP") Join message to the first-hop router.

Mathis does not disclose how the client devices 102 are configured and does not disclose "said message detection data comprising at least one individual address corresponding to said digital broadcast receiver and, for each individual address, at least one associated key."

Thus, claims 8 and 47 are allowable over the prior art of record.

Accordingly, claims 1-3, 5, 6, 8-10, 12, 14, 15, 17, 28-31, 41, 42, 44,45, and 47-49 are patentable over the prior art of record.

New claims 50-56 are also believed to be patentable over the prior art of record at least for the reasons provided above.

The Patent Office is respectfully requested to reconsider and remove the rejections of claims 1-10, 12, 14-17, and 23-49 under 35 U.S.C. 103(a) based on Nagaoka in view of Ching (or, Syed), whether or not in combination with Thornton, Syed, and/or Mathis, and to allow all of the pending claims 1-3, 5, 6, 8-10, 12, 14, 15, 17, 28-31, 41, 42, 44, 45, and 47-56 as now presented for examination. An early notification of the allowability of claims 1-3, 5, 6, 8-10, 12, 14, 15, 17, 28-31, 41, 42, 44, 45, and 47-56 is earnestly solicited.